(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－143443

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｃ
	3/06	３０４		3/06	３０４Ｈ
	13/10	３４０		13/10	３４０Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）

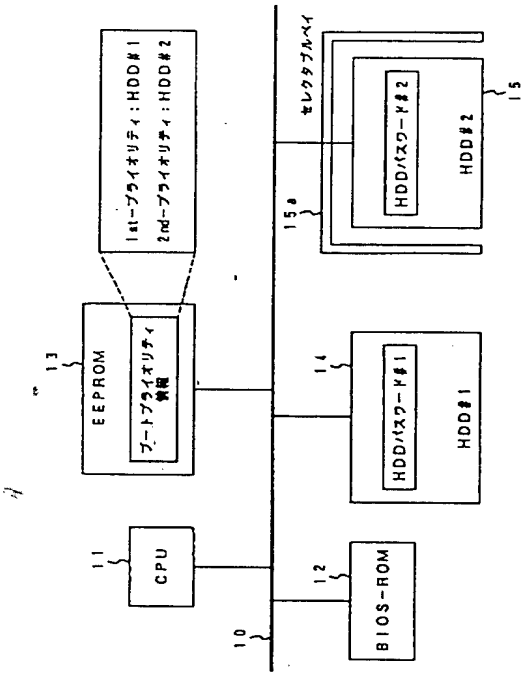
(21)出願番号　特願平8－305016

(22)出願日　平成８年(1996)11月15日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　前田　真弓
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　コンピュータシステムおよび同システムにおけるハードディスクパスワード制御方法

(57)【要約】
【課題】複数のハードディスクドライブが搭載されたシステムに最適なＨＤＤパスワードチェック処理を実現する。
【解決手段】システムのパワーオン時にＣＰＵ１１によって最初に実行されるＰＯＳＴは、１ｓｔ－プライオリティのＨＤＤ１４がＨＤＤパスワードチェックによりそれがアクセス可能状態となれば、２ｎｄ－プライオリティのＨＤＤ１５の状態とは無関係にブートストラップを実行する。したがって、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるＨＤＤ１４のパスワードさえ知っていればコンピュータを利用することができるようになる。また、２ｎｄ－プライオリティのＨＤＤ１５についても正当なパスワードが入力された場合にはそのデータの読み出しや更新を行うことができる。



【特許請求の範囲】

【請求項１】　パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、

前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第１のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第１のハードディスクドライブ以外の他のハードディスクドライブそれぞれの状態とは無関係に、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコンピュータシステム。

【請求項２】　前記第１のハードディスクドライブのデータロック機能が解除されないとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項１記載のコンピュータシステム。

【請求項３】　パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、

前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第１のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコンピュータシステム。

【請求項４】　前記複数のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項２記載のコンピュータシステム。

【請求項５】　コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、

パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、

前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第１のハードディスクドライブが動作可能で、且つ前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在するドライブであるか否かを判別する手段と、

前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコン

ピュータシステム。

【請求項６】　前記データロック機能が解除されないドライブが前記コンピュータ本体に存在しているとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項５記載のコンピュータシステム。

【請求項７】　パスワードが設定可能に構成され、パスワードが設定されているときそのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第１のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行した後、前記コンピュータシステムのブートストラップを実行することを特徴とするパスワード制御方法。

【請求項８】　前記第１のハードディスクドライブのデータロック機能が解除されないとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項７記載のパスワード制御方法。

【請求項９】　パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第１のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行した後、前記第１のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるか否かを検出し、

前記第１のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行することを特徴とするパスワード制御方法。

【請求項１０】　前記第１のハードディスクドライブのデータロック機能が解除されないとき、および前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項９記載のパスワード制御方法。

【請求項１１】　コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第１のハードディスクドライブが動作可能状態であるとき、前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行し、

前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在するドライブであるか否かを判別し、

前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラ

ップを実行することを特徴とするパスワード制御方法。
【請求項１２】　前記第１のハードディスクドライブのデータロック機能が解除されないとき、および前記他のハードディスクドライブの中のデータロック機能が解除されないドライブが前記コンピュータ本体に存在しているとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項１１記載のパスワード制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明はコンピュータシステムおよびパスワード制御方法に関し、特にハードディスクドライブに設定されるＨＤＤパスワードを用いてそのデータのセキュリティーを保持するコンピュータシステムおよびＨＤＤパスワードの制御方法に関する。
【０００２】
【従来の技術】近年、ノートブックタイプおよびサブノートタイプの各種ポータブルコンピュータが開発されている。この種のポータブルコンピュータはその持ち運びが用意であるため、コンピュータ本体ごと盗難される危険がある。この場合、コンピュータ本体からその本体に内蔵されているハードディスクドライブを取り外し、そしてそのハードディスクドライブを他のコンピュータからアクセスすることなどによって、そのハードディスクドライブ内のデータを不正に読み出すことが可能となる。特に、コンピュータ本体に取り外し自在に装着できるパック型のハードディスクドライブについては、コンピュータ本体から簡単にハードディスクドライブを取り外すことができるため、不正なデータ読み出し操作やデータ書き換え操作を行うことはきわめて容易である。
【０００３】そこで、最近では、ドライブ自体にパスワード（ＨＤＤパスワード）が設定可能に構成され、ユーザから正当なパスワードが入力されるまでデータアクセス操作を禁止するというデータロック機能を持つハードディスクドライブが開発され始めている。このハードディスクドライブのデータロック機能の仕組みは、ＵＳＰ５，３７５，２４３号公報に開示されている。現在では、このＵＳＰ５，３７５，２４３号公報と同等のデータロック機能はＩＤＥインタフェースを持つハードディスクドライブの標準仕様としてその策定作業が進められている。
【０００４】この種のハードディスクドライブを使用した典型的なＨＤＤパスワードチェック処理では、まず、ソフトウェアの制御により、ハードディスクドライブにＨＤＤパスワードが設定されているか否かが調べられ、設定されていれば、ユーザに対してパスワードの入力が促される。ユーザからパスワードが入力されると、その入力パスワードとハードディスク内のＨＤＤパスワードとの照合がソフトウェアまたはハードディスクドライブ自体によって行われ、一致すると、ハードディスクドライブのデータロック機能が自動的またはソフトウェア制御の下で解除され、そのデータアクセス操作が可能となる。
【０００５】したがって、データロック機能を持つハードディスクドライブを使用した場合には、正当なパスワードを入力しない限り、その記憶データを読み出したり、更新することが禁止されるため、そのデータ内容の機密性を保持することができる。
【０００６】
【発明が解決しようとする課題】ところで、最近では、ポータブルコンピュータにおいてもデスクトップ型コンピュータと同等の性能および拡張性が要求されており、２台目のハードディスクドライブとＣＤ－ＲＯＭドライブとを選択的に増設可能なセレクタブルベイを有するポータブルコンピュータや、ドッキングステーション等と称される専用の拡張ユニットを用いてその拡張ベイに収容されているハードディスクドライブを２台目のハードディスクドライブとして使用可能なポータブルコンピュータなどが開発されている。
【０００７】このようにコンピュータ本体やドッキングステーションに増設されるハードディスクドライブについても、前述したデータロック機能を持つタイプのハードディスクドライブを使用することができる。
【０００８】しかし、前述した従来のパスワードチェック機能は、ハードディスクドライブ毎にＨＤＤパスワードを個々に照合するだけのものであるため、システムに搭載されているどのハードディスクドライブに対しても共通のパスワードチェックが行われる。このため、オペレーティングシステムを格納したハードディスクであるか否かや、コンピュータ本体とドッキングステーションのどちらに接続されたハードディスクドライブであるかなど、ハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したセキュリティー管理を行うことはできなかった。
【０００９】この発明はこのような点に鑑みてなされたもので、データロック機能を有する複数のハードディスクドライブを使用可能な環境下においてそれらハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したパスワードチェック処理を実行できるようにし、システム全体の総合的なセキュリティーレベルを向上することが可能なコンピュータシステムおよびＨＤＤパスワード制御方法を提供することを目的とする。
【００１０】
【課題を解決するための手段】請求項１に係る発明は、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピ

ュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第１のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第１のハードディスクドライブ以外の他のハードディスクドライブそれぞれの状態とは無関係に、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【００１１】このコンピュータシステムにおいては、コンピュータシステムがパワーオンされた時に最初に実行されるＰＯＳＴ（Ｐｏｗｅｒ－Ｏｎ　Ｓｅｌｆ　Ｔｅｓｔ）プログラムなどを用いて、以下のＨＤＤパスワード制御処理が行われる。すなわち、コンピュータシステムがパワーオンされると、まず、ＰＯＳＴプログラムが、複数のハードディスクドライブの中でブート優先順位が最も高いハードディスクドライブ、つまりブートデバイスとして使用されるハードディスクドライブについて、パスワードの設定の有無が調べられる。パスワードが設定されていれば、パスワード入力用ウインドウの表示などによって、パスワードの入力がユーザに促される。パスワードが入力されると、その入力パスワードとハードディスクドライブに設定されているパスワードとの一致の有無がＰＯＳＴ、あるいはハードディスクドライブ内部で調べられ、一致したときのみデータロック状態が解除される。これにより、ブートデバイスとして使用されるハードディスクドライブについては、パスワードが設定されていないか、あるいは正当なパスワードが入力された時にアクセス可能状態となる。ブートデバイス以外の他のハードディスクドライブそれぞれに対しても、同様にしてパスワード設定の有無の検出、および入力パスワードに基づいてデータロック状態を解除するためのパスワード制御処理が実行される。そして、この後、ブートデバイスとして使用されるハードディスクドライブがアクセス可能状態であるならば、他のハードディスクドライブそれぞれの状態によらず、ブートストラップが実行され、ブートデバイスとして使用されるハードディスクドライブからオペレーティングシステムが起動される。

【００１２】このように、ブートデバイスとして使用されるハードディスクドライブがアクセス可能状態であれば、他のハードディスクドライブそれぞれの状態とは無関係にブートストラップを実行することにより、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるハードディスクドライブのパスワードさえ知っていればコンピュータを利用することができるようになる。この場合、他のハードディスクドライブについても正当なパスワードが入力されたものついてはそのデータの読み出しや更新を行うことができ、また正当なパスワードが入力されなかったものについてはブート後においてもそのデータ内容の読み出しや更新は禁止されることになる。したがって、ハードディスクドライブそれぞれの用途の違いを考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティーレベルの向上とユーザの利便性とを両立することができる。

【００１３】また、請求項２に係る発明においては、ブートデバイスとして使用されるハードディスクドライブに対応する正当なパスワードが入力されず、そのデータロック機能を解除できなかった場合には、そのままブートストラップ処理に移行してもそのハードディスクドライブからオペレーティングシステムを起動することはできないので、他のハードディスクドライブに対するパスワード制御処理およびブートストラップ処理を行うことなく、ブートデバイスに対する正当なパスワードが入力されなかった時点でコンピュータシステムを強制的にパワーオフすることを特徴とする。

【００１４】ブートストラップ処理では、通常、複数のハードディスクドライブの中で最もブート優先順位の高いハードディスクドライブからオペレーティングシステムが起動されるが、多くのコンピュータでは、ブートストラップ処理時にフロッピーディスクが装着されていると、そのフロッピーディスクからオペレーティングシステムが起動されるように構成されている。したがって、請求項２のようにブートストラップ処理が実行される前にシステムを強制的にパワーオフすることは、ブートデバイスとして使用されるハードディスクドライブのパスワードを知らない人、つまり不正者によるフロッピーディスクなどを用いたブートストラップ処理の防止を図ることができる。

【００１５】また、請求項３に係る発明は、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第１のハードデ

ィスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第１のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【００１６】このコンピュータシステムにおいては、セキュリティーレベルをさらに向上させるために、ブートデバイスとして使用されるハードディスクドライブのみならず、それ以外の他のすべてのハードディスクドライブがアクセスが可能であるときのみブートストラップが実行される。したがって、すべてのハードディスクドライブについて正しいパスワードを知っているユーザに対してのみコンピュータの使用を許可することができる。

【００１７】また、請求項５に係る発明は、コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第１のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第１のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第１のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第１のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第１のハードディスクドライブが動作可能で、且つ前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在するドライブであるか否かを判別する手段と、前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【００１８】このコンピュータシステムにおいては、ブートデバイス以外の他のハードディスクドライブが拡張ユニットに存在するものであるか、コンピュータ本体に存在するものであるかによってブート制御が切り替えられ、拡張ユニットに存在するものであればそのデータロック状態を解除できない場合であってもブートストラップ処理は実行される。これにより、例えばネットワーク接続された拡張ユニットがオフィス内に幾つか設置されており、その拡張ユニットにユーザ自身のコンピュータを装着してデータ通信などを行う場合は、拡張ユニット内に設けられた他人のハードディスクドライブの機密性を維持したまま、拡張ユニットの通信機能を利用するといった運用が可能となる。

【００１９】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図１には、この発明の一実施形態に係るコンピュータシステムの構成が示されている。このコンピュータシステムはノートブックタイプのポータブルコンピュータであり、そのコンピュータ本体には、図示のように、システムバス１０、ＣＰＵ１１、ＢＩＯＳ－ＲＯＭ１２、ＥＥＰＲＯＭ１３、およびハードディスクドライブ（ＨＤＤ＝１）１４が内蔵されている。さらに、そのコンピュータ本体には、ハードディスクドライブまたはＣＤ－ＲＯＭドライブを選択的に増設するためのセレクタブルベイ１５ａが設けられており、この実施形態では、セレクタブルベイ１５ａには２台目のハードディスクドライブ（ＨＤＤ＝２）１５が収容されている。

【００２０】ハードディスクドライブ（ＨＤＤ＝１）１４はＩＤＥ規格のＡＴＡドライブであり、データロック機能を有している。このデータロック機能は、パスワード設定プログラム等を用いてユーザがハードディスクドライブ（ＨＤＤ＝１）１４内にＨＤＤパスワード＝１を予め登録しておくことによって有効となり、ＨＤＤパスワード＝１と一致するパスワードが入力された時に解除される。データロック機能が有効な状態においては通常のデータリード／ライトに関するコマンドは一切受け付けられず、これによりデータアクセス操作の実行が禁止される。

【００２１】ハードディスクドライブ（ＨＤＤ＝２）１５もハードディスクドライブ（ＨＤＤ＝１）１４と同じデータロック機能を有しており、ＨＤＤパスワード＝２を設定しておくことにより、そのパスワードが入力されるまではデータアクセス操作を禁止することができる。

【００２２】ＣＰＵ１１は、このシステム全体の動作を制御するものであり、オペレーティングシステムおよび

各種アプリケーションプログラムを初め、ＢＩＯＳ－ＲＯＭ１２に格納されたシステムＢＩＯＳを実行する。このシステムＢＩＯＳには、コンピュータシステムのパワーオン時に最初に実行されるＰＯＳＴプログラムが含まれており、ＨＤＤのデータロック機能を利用するためのパスワード制御処理はこのＰＯＳＴプログラムによって実行される。

【００２３】パスワード制御処理はハードディスクドライブ１４，１５に記憶されているデータやプログラムの不正使用および書き換えを防止するためのものであるが、この実施形態では、さらに、セキュリティーレベルの向上のために、ブートデバイスとして使用されるハードディスクドライブのデータロックが解除できない場合はブートストラップを実行せずにシステムを強制的にパワーオフする仕組みが設けられている。パスワード制御処理の詳細な手順は図３乃至図５のフローチャートを参照して後述する。

【００２４】ハードディスクドライブ１４，１５のどちらをブートデバイスとして使用するかは、ＥＥＰＲＯＭ１３に設定されているブート優先順位情報によって決定される。このブート優先順位情報はオペレーティングシステムを起動するハードディスクの順番を規定するものであり、環境設定プログラムなどを用いることによりユーザが自由に書き換えることができる。図１のブート優先順位情報においてはハードディスクドライブ１４，１５の順でブート優先順位が割り当てられており、この場合には、ハードディスクドライブ１４が１ｓｔープライオリティのＨＤＤ（ブートデバイス）、ハードディスクドライブ１４が２ｎｄープライオリティのＨＤＤとなる。

【００２５】この実施形態のパスワード制御処理は、以上のようなシステム構成、つまり、以下の条件下で動作することを前提としている。

（１）データロック機能を有するハードディスクドライブをサポートするシステムである。

（２）データロック機能を有するハードディスクドライブが２台またはそれ以上接続されている。

（３）２台またはそれ以上のハードディスクドライブに対してブート優先順位を割り当てることができ、１ｓｔープライオリティのＨＤＤと２ｎｄープライオリティ以降のＨＤＤが明確化されている。

【００２６】以上の条件は、２台目以降のハードディスクドライブをコンピュータ本体ではなく、図２に示されているように、ドッキングステーション３０に収容して使用する場合でも満足される。

【００２７】図２のシステムにおいては、コンピュータ本体を取り外し自在に装着できるドッキングステーション３０のセレクタブルベイ１５ａにハードディスクドライブ１５が収容されている。コンピュータ本体をコネクタ２０を介してドッキングステーション３０に接続した場合には、コンピュータ本体は２台のハードディスクドライブを持つシステム構成に機能拡張されることになる。

【００２８】また、図１のポータブルコンピュータ本体を図２のドッキングステーション３０に接続し、３台のハードディスクドライブを持つシステム構成として使用することも可能である。

【００２９】次に、図３のフローチャートを参照して、ＰＯＳＴプログラムによって実行されるパスワード制御処理の第１の例を説明する。コンピュータがパワーオンされると、ＣＰＵ１１によって最初にＰＯＳＴプログラムが実行され、そのＰＯＳＴプログラムの制御の下でメモリおよびハードウェアテストが行われ、その処理が正常終了するとブートストラップが開始される。パスワード制御処理はシステムに接続されているハードディスクドライブのテストおよび初期化時に以下の手順で実行される。

【００３０】ＰＯＳＴプログラムは、まず、ＥＥＰＲＯＭ１３のブート優先順位情報からブートデバイスとなるハードディスクドライブ（１ｓｔープライオリティのＨＤＤ１４）を認識し、その１ｓｔープライオリティのＨＤＤ１４にＨＤＤパスワードが設定されているか否かを調べる（ステップＳ１０１）。これは、１ｓｔープライオリティのＨＤＤ１４がデータロック状態か否かを問い合わせるステータスリードコマンドをＨＤＤ１４に発行することによって行うことができる。１ｓｔープライオリティのＨＤＤ１４にＨＤＤパスワードが設定されている場合は、ＰＯＳＴプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ１０２）。

【００３１】パスワードが入力されると、ＰＯＳＴプログラムは、１ｓｔープライオリティのＨＤＤ１４から読み取ったＨＤＤパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ１０３）。正しいならば、ＰＯＳＴプログラムは、１ｓｔープライオリティのＨＤＤ１４にデータロック解除コマンドを送ることによりＨＤＤ１４にデータロック状態を解除させ、ＨＤＤ１４をデータアクセス可能状態にする（ステップＳ１０５）。入力パスワードが正しくない場合には、１ｓｔープライオリティのＨＤＤ１４のデータロック状態は解除できないので、ＨＤＤ１４からオペレーティングシステムを起動することはできない。このため、ＰＯＳＴプログラムは、セキュリティーレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップＳ１０４）。このようにブートストラップ処理を実行する前にシステムをパワーオフすることにより、不正者によるフロッピーディスクなどを用いたオペレーティングシステムの起動を防止することができる。

【００３２】ＨＤＤ１４がパスワード照合機能を持つ場

合には、ステップＳ１０３ではＰＯＳＴプログラムはＨＤＤ１４にパスワードを入力するだけで良く、またパスワードが一致した場合にはＨＤＤ１４内でデータロック機能が自動的に解除されるので、ステップＳ１０５の処理は不要となる。パスワードの一致の有無は、ＰＯＳＴプログラムがＨＤＤ１４にステータスリードコマンドを発行してデータロック状態か否かを調べることなどによって認識することができる。

【００３３】ＨＤＤ１４のデータロック状態が解除されたとき、またはＨＤＤ１４にＨＤＤパスワードが設定されていなかったときは、２ｎｄ－プライオリティのＨＤＤ１５に対して同様の処理が実行される。

【００３４】すなわち、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されているか否かを調べる（ステップＳ１０６）。２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されている場合は、ＰＯＳＴプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ１０７）。パスワードが入力されると、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５から読み取ったＨＤＤパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ１０８）。正しいならば、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にデータロック解除コマンドを送ることによりＨＤＤ１５にデータロック状態を解除させ、ＨＤＤ１５をデータアクセス可能状態にする（ステップＳ１０９）。ステップＳ１０８およびステップＳ１０９は、前述したＨＤＤ１４の場合と同様にし、ＨＤＤ１５自体のパスワード照合機能を利用して行うこともできる。

【００３５】この後、ＰＯＳＴプログラムは、ＨＤＤ１５のデータロック状態が解除されたか否か、およびＨＤＤ１５にパスワードが設定されていたか否かに関わらず、ブートストラップ処理を実行する（ステップＳ１１０）。このブートストラップ処理はＰＯＳＴプログラムによって起動されるシステムＢＩＯＳ内のブートアッププログラムによって実行され、１ｓｔ－プライオリティのＨＤＤ１４からオペレーティングシステムが主記憶上にロードされる。

【００３６】以上のように、図３のパスワード制御処理の手順においては、１ｓｔ－プライオリティのＨＤＤ１４がアクセス可能状態であれば、２ｎｄ－プライオリティのＨＤＤ１５の状態とは無関係にブートストラップを実行される。したがって、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるＨＤＤ１４のパスワードさえ知っていればコンピュータを利用することができるようになる。また、２ｎｄ－プライオリティのＨＤＤ１５についても正当なパスワードが入力された場合にはそのデータの読み出しや更新を行うことができ、また正当なパスワードが入力されなかった場合にはブート後においてもそのデータ内容の読み出しや更新は禁止されることになる。したがって、ハードディスクドライブ１４，１５それぞれのブート優先順位を考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティーレベルの向上とユーザの利便性とを両立することができる。

【００３７】次に、図４のフローチャートを参照して、ＰＯＳＴプログラムによって実行されるパスワード制御処理の第２の例を説明する。このパスワード制御処理は、図３の処理よりもさらにセキュリティーレベルを高めることを目的としており、１ｓｔ－プライオリティのＨＤＤ１４および２ｎｄ－プライオリティのＨＤＤ１５の双方がアクセス可能状態になったときに初めてブートストラップを実行する構成である。

【００３８】すなわち、コンピュータがパワーオンされると、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４にＨＤＤパスワードが設定されているか否かを調べ（ステップＳ２０１）、ＨＤＤ１４にＨＤＤパスワードが設定されている場合は、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ２０２）。パスワードが入力されると、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４から読み取ったＨＤＤパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ２０３）。正しいならば、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４にデータロック解除コマンドを送ることによりＨＤＤ１４にデータロック状態を解除させ、ＨＤＤ１４をデータアクセス可能状態にする（ステップＳ２０５）。入力パスワードが正しくない場合には、１ｓｔ－プライオリティのＨＤＤ１４のデータロック状態は解除できないので、ＨＤＤ１４からオペレーティングシステムを起動することはできない。このため、ＰＯＳＴプログラムは、セキュリティーレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップＳ２０４）。

【００３９】ＨＤＤ１４のデータロック状態が解除されたとき、またはＨＤＤ１４にＨＤＤパスワードが設定されていなかったときは、２ｎｄ－プライオリティのＨＤＤ１５に対して以下の処理が行われる。

【００４０】すなわち、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されているか否かを調べる（ステップＳ２０６）。２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されている場合は、ＰＯＳＴプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ２０７）。パスワードが入力されると、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５から読み取ったＨＤＤパスワードと

ユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ２０８）。正しいならば、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にデータロック解除コマンドを送ることによりＨＤＤ１５にデータロック状態を解除させ、ＨＤＤ１５をデータアクセス可能状態にする（ステップＳ２０９）。

【００４１】この後、ＰＯＳＴプログラムは、ＨＤＤ１５のデータロック状態が解除されたか、あるいはＨＤＤ１５にパスワードが設定されていたかった場合、つまりＨＤＤ１４およびＨＤＤ１５の双方がアクセス可能状態であることを条件に、ブートストラップ処理を実行する（ステップＳ２１０）。１ｓｔ－プライオリティのＨＤＤ１４がアクセス可能状態であっても、２ｎｄ－プライオリティのＨＤＤ１５のデータロック状態が解除できない場合は、システムが強制的にパワーオフされる（ステップＳ２１１）。

【００４２】次に、図５のフローチャートを参照して、ＰＯＳＴプログラムによって実行されるパスワード制御処理の第３の例を説明する。このパスワード制御処理では、１ｓｔ－プライオリティのＨＤＤがアクセス可能状態で、且つ２ｎｄ－プライオリティ以降のＨＤＤの中にデータロック状態を解除できないＨＤＤがある場合に、そのＨＤＤがドッキングステーションとコンピュータ本体のどちらに設けられているものであるかが調べられ、ドッキングステーションに設けられているものであったときにブートストラップが許可される。

【００４３】すなわち、コンピュータがパワーオンされると、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４にＨＤＤパスワードが設定されているか否かを調べ（ステップＳ３０１）、ＨＤＤ１４にＨＤＤパスワードが設定されている場合は、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ３０２）。パスワードが入力されると、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４から読み取ったＨＤＤパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ３０３）。正しいならば、ＰＯＳＴプログラムは、１ｓｔ－プライオリティのＨＤＤ１４にデータロック解除コマンドを送ることによりＨＤＤ１４にデータロック状態を解除させ、ＨＤＤ１４をデータアクセス可能状態にする（ステップＳ３０５）。入力パスワードが正しくない場合には、１ｓｔ－プライオリティのＨＤＤ１４のデータロック状態は解除できないので、ＨＤＤ１４からオペレーティングシステムを起動することはできない。このため、ＰＯＳＴプログラムは、セキュリティーレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップＳ３０４）。

【００４４】ＨＤＤ１４のデータロック状態が解除されたとき、またはＨＤＤ１４にＨＤＤパスワードが設定されていなかったときは、２ｎｄ－プライオリティのＨＤＤ１５に対して以下の処理が行われる。

【００４５】すなわち、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されているか否かを調べる（ステップＳ３０６）。２ｎｄ－プライオリティのＨＤＤ１５にＨＤＤパスワードが設定されている場合は、ＰＯＳＴプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップＳ３０７）。パスワードが入力されると、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５から読み取ったＨＤＤパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップＳ３０８）。正しいならば、ＰＯＳＴプログラムは、２ｎｄ－プライオリティのＨＤＤ１５にデータロック解除コマンドを送ることによりＨＤＤ１５にデータロック状態を解除させ、ＨＤＤ１５をデータアクセス可能状態にする（ステップＳ３０９）。そして、ブートストラップ処理が実行される（ステップＳ３１２）。

【００４６】一方、２ｎｄ－プライオリティのＨＤＤ１５のデータロック状態が解除できない場合には、ＰＯＳＴプログラムは、そのＨＤＤ１５がコンピュータ本体とドッキングステーションのどちらに設けられているかを検出し（ステップＳ３１０）、コンピュータ本体に設けられたものであれば、その時点でシステムを強制的にパワーオフする（ステップＳ３１１）。また、データロック状態が解除できないＨＤＤ１５がドッキングステーションに設けられたものである場合には、ブートストラップ処理が実行される（ステップＳ３１２）。

【００４７】このように、ブートデバイス以外の他のハードディスクドライブがドッキングステーションに存在するものであるか、コンピュータ本体に存在するものであるかによってブート制御を切り替え、ドッキングステーションに存在するものであればそのデータロック状態を解除できない場合であってもブートストラップ処理を実行することにより、例えばネットワーク接続されたドッキングステーションにユーザ自身のコンピュータ本体を装着してデータ通信などを行う場合は、ドッキングステーション内に設けられた他人のハードディスクドライブの機密性を維持したまま、そのドッキングステーションの通信機能を利用するといった運用が可能となる。

【００４８】

【発明の効果】以上説明したように、この発明によれば、データロック機能を有する複数のハードディスクドライブを使用可能な環境下においてそれらハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティーレベルを向上することが可能とかなる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係るコンピュータシステムの構成を示すブロック図。

【図２】同実施形態のコンピュータシステムの他の構成例を示すブロック図。

【図３】同実施形態で使用されるＨＤＤパスワード制御処理の第１の手順を示すフローチャート。

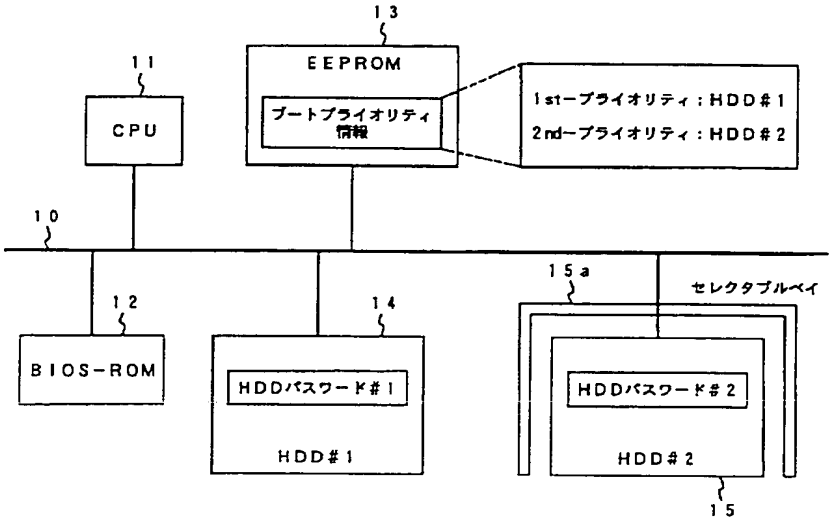
【図４】同実施形態で使用されるＨＤＤパスワード制御処理の第２の手順を示すフローチャート。

【図５】同実施形態で使用されるＨＤＤパスワード制御処理の第３の手順を示すフローチャート。

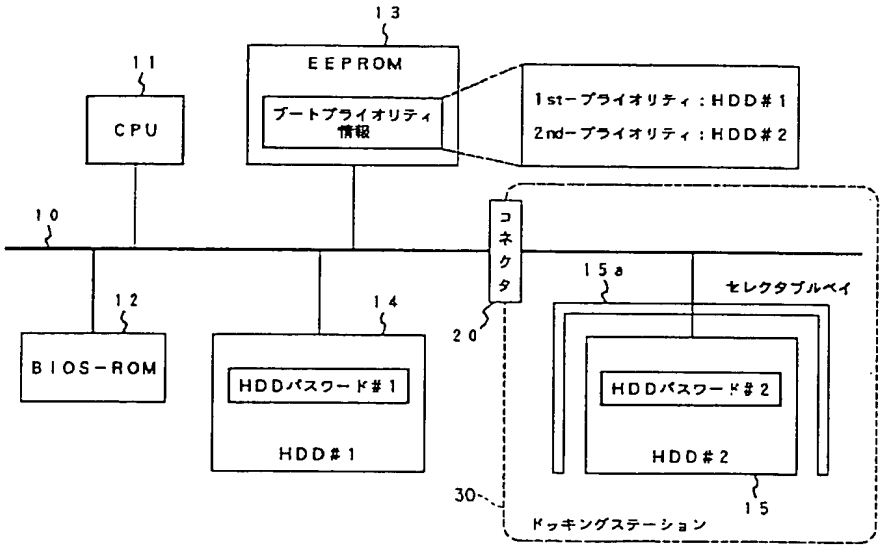
【符号の説明】

１１…ＣＰＵ、１２…ＢＩＯＳ－ＲＯＭ、１３…ＥＥＰＲＯＭ、１４…１ｓｔ－プライオリティのＨＤＤ、１５…２ｎｄ－プライオリティのＨＤＤ、１５ａ…セレクタブルベイ、３０…ドッキングステーション。

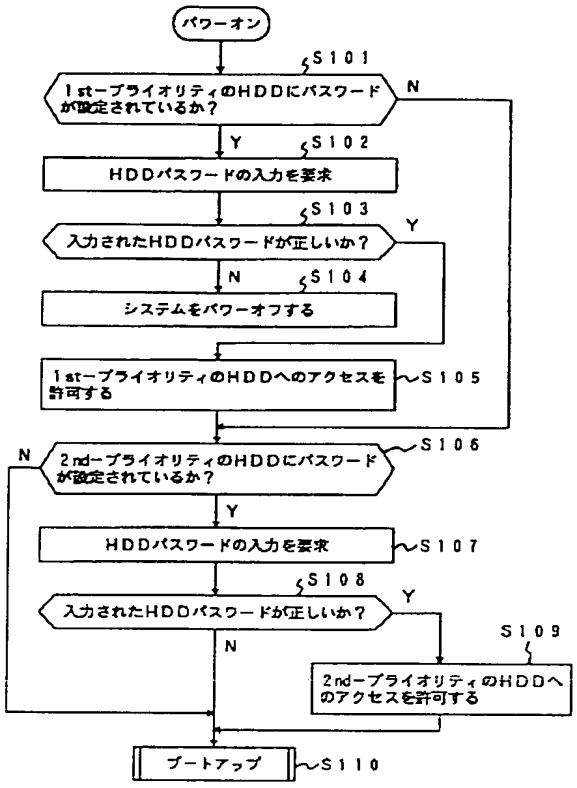
【図１】



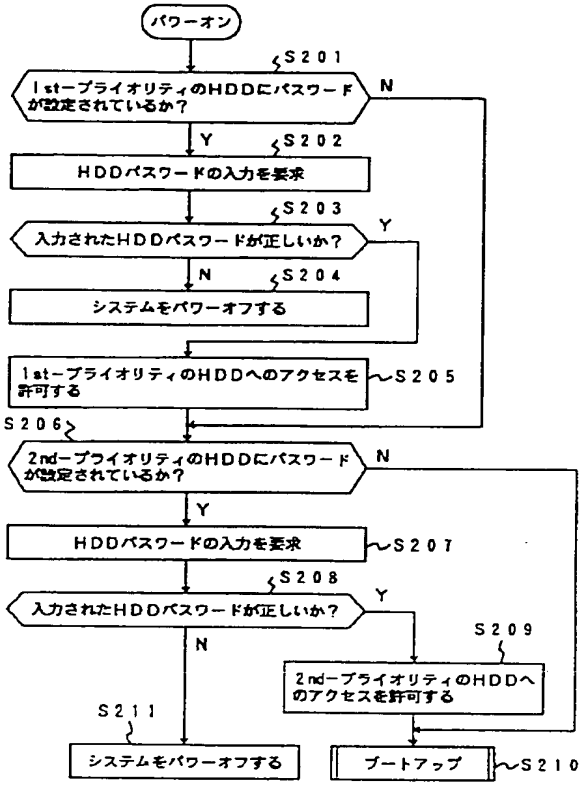
【図２】



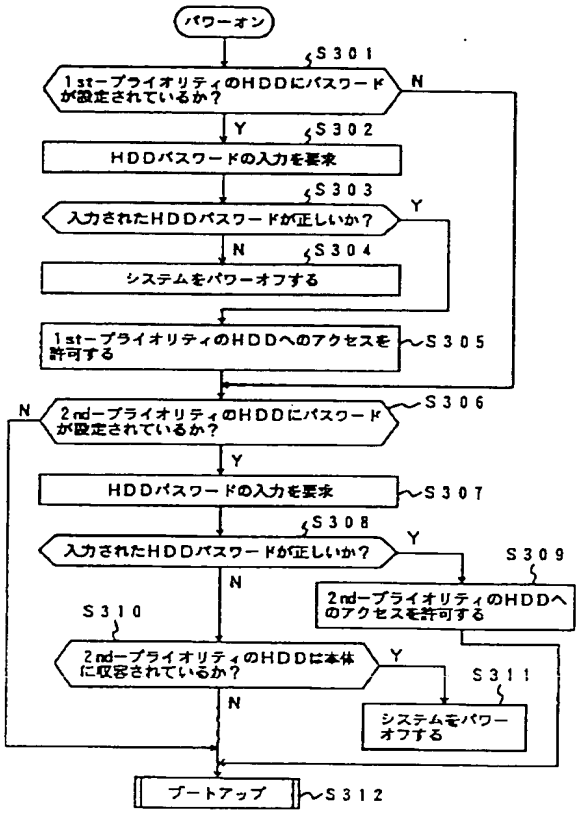
【図３】


パワーオン
S101
1st-プライオリティのHDDにパスワードが設定されているか？
N
Y
S102
HDDパスワードの入力を要求
S103
入力されたHDDパスワードが正しいか？
Y
N
S104
システムをパワーオフする
1st-プライオリティのHDDへのアクセスを許可する
S105
S106
N
2nd-プライオリティのHDDにパスワードが設定されているか？
Y
HDDパスワードの入力を要求
S107
S108
入力されたHDDパスワードが正しいか？
Y
S109
N
2nd-プライオリティのHDDへのアクセスを許可する
ブートアップ
S110

【図４】


パワーオン
S201
1st-プライオリティのHDDにパスワードが設定されているか？
N
Y
S202
HDDパスワードの入力を要求
S203
入力されたHDDパスワードが正しいか？
Y
N
S204
システムをパワーオフする
1st-プライオリティのHDDへのアクセスを許可する
S205
S206
2nd-プライオリティのHDDにパスワードが設定されているか？
N
Y
HDDパスワードの入力を要求
S207
S208
入力されたHDDパスワードが正しいか？
Y
S209
N
2nd-プライオリティのHDDへのアクセスを許可する
S211
システムをパワーオフする
ブートアップ
S210

【図５】


パワーオン
S301
1st-プライオリティのHDDにパスワードが設定されているか？
N
Y
S302
HDDパスワードの入力を要求
S303
入力されたHDDパスワードが正しいか？
Y
N
S304
システムをパワーオフする
1st-プライオリティのHDDへのアクセスを許可する
S305
2nd-プライオリティのHDDにパスワードが設定されているか？
S306
N
Y
HDDパスワードの入力を要求
S307
S308
入力されたHDDパスワードが正しいか？
Y
S309
N
2nd-プライオリティのHDDへのアクセスを許可する
S310
2nd-プライオリティのHDDは本体に収容されているか？
Y
S311
N
システムをパワーオフする
ブートアップ
S312